Problem 1. For all integers $a, b, c > 0$. Show that:

(a) $\gcd(ca, cb) = c \cdot \gcd(a, b)$ and $\text{lcm}(ca, cb) = c \cdot \text{lcm}(a, b)$

(b) $d = \gcd(a, b) \neq 0$ if and only if $\gcd(a/d, b/d) = 1$

**Hint:** recall from the lecture, if $d = \gcd(a, b)$ then we can express $d$ as a linear combination of $a, b$, namely, $ax + by = d$ for some $x, y \in \mathbb{Z}$

---

part a: $\text{lcm}(ca, cb) = c \cdot \text{lcm}(a, b)$, let $d = \text{lcm}(ca, cb)$ and $e = c \cdot \text{lcm}(a, b)$

to show: $d \leq e$ (1), $e \leq d$ implies $d = e$ (2)

(1) On the one hand, $\text{lcm}(a, b) = ax = by$ for some integers $x, y$
$c \cdot \text{lcm}(a, b) = c\cdot ax = c\cdot by = e$ --> $e$ is a common multiple of both $ca$ and $cb$
since $d = \text{lcm}(ca, cb)$, therefore, $d \leq e$

(2) On the other hand, $\text{lcm}(ca, cb) = cax = cby = d$ for some integers $x, y$
given $d = cax = cby$ => $d/c = ax = by$ which implies that $d/c$ is a common multiple of both $a$ & $b$
$\text{lcm}(a, b) \leq d/c$ => $c \cdot \text{lcm}(a, b) \leq d$ => $e \leq d$

Hence, $e = d$ ./.

first part: $d = \gcd(ca, cb)$ and $e = c \cdot \gcd(a, b)$, strategy: $d \geq e$; $e \geq d$ --> $d = e$

part b: 
"=" given: $d = \gcd(a, b)$, to show $\gcd(a/d, b/d) = 1$

express $d$ as: $ax + by = d$ for some integers $x, y$

$\Rightarrow a/d \cdot x + b/d \cdot y = 1$ --> $\gcd(a/d, b/d) = 1$

"$\leq$" given $\gcd(a/d, b/d) = 1$, to show $d = \gcd(a, b)$

$\gcd(a/d, b/d) = 1$ --> $a/d \cdot x + b/d \cdot y = 1$

$\Rightarrow ax + by = d$
suppose, for the sake of contradiction, we a common multiple $c > d$

$(ax)/c + (by)/c = d/c$ (contradiction because $d/c$ is not an integer)
Problem 2. Let $a, b, n \in \mathbb{Z}$ with $n > 0$ and $a \equiv b \pmod{n}$ Show that $\gcd(a, n) = \gcd(b, n)$. 
Problem 3. Let $a \in \mathbb{Z}$, show that: $a^2 \not\equiv 2 \pmod{4}$ or $a^2 \not\equiv 3 \pmod{4}$

**Hint:** consider we have $a \equiv n \pmod{4}$, then what are the possible values for $n$? Then, for each $n$, how can we express $a$ in terms of some $x \in \mathbb{Z}$? At this point, what is special about $a^2$ in terms of $x$?